

EDITORS' PICK | 123,247 views | May 8, 2020, 03:51am EDT

Zoom Security: You Need To Know About These 3 New Features



Kate O'Flaherty Senior Contributor 

[Cybersecurity](#)

I'm a cybersecurity journalist.



From May 9, Zoom hopes to eliminate Zoom bombing and other security problems with a bunch of new ... [\[+\]](#) SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES

Video conferencing app Zoom has seen a [massive surge in users](#) as many people continue to stay at home during the COVID-19 crisis.

But many new Zoom users are just normal people using the platform to talk to friends or take an exercise class—I'm one of them.

This sudden surge in Zoom users beyond the app's traditional business base has led to major security issues such as "[Zoom bombing](#)," which sees uninvited guests join your meeting or chat. From May 9, [Zoom](#) hopes to eliminate this and other security problems with a bunch of new features for basic and free accounts.

Here are the three features arriving tomorrow that you need to know about:

MORE FROM FORBES

Beware Zoom Users: Here's How People Can 'Zoom-Bomb' Your Chat

By [Kate O'Flaherty](#)

Passwords now required for *all* meetings

Most Popular In: [Cybersecurity](#)



Beware—100 Million Android Users Have Now Installed This Dangerous Chinese 'Spyware'

Gamers Beware: Stealthy Malware Steals Your Discord Password And Attacks Your Friends

Don't Press Windows 10 2004 'Update Now' Button, Microsoft Warns Some Users

If you don't have a meeting password, you're not safe. It means that if someone knows your Meeting ID or has a link to your chat, they can simply join it—also known as Zoom bombing. Many people also share their Zoom Meeting IDs on social media, which is a definite no-no as it leaves your meetings wide open for anyone to crash.

So from May 9, Zoom wants to make the chance of this happening even smaller by requiring a password for all meetings. This includes new meetings, previously scheduled meetings and those using a personal meeting ID.

Waiting Rooms turned on by default

Another Zoom problem that can allow video chat gatecrashers is the ability to simply enter the meeting without being let in by the host. Zoom has a feature called [Waiting Rooms](#) to allow the host to manually let people into the meeting, but not everyone was using it. In another move to stop Zoom bombers, Zoom will now make Waiting Rooms turned on by default. It means it will take slightly longer to enter your meeting, but it's certainly worth it for the security and privacy benefits.

MORE FROM FORBES

Zoom Buys Keybase In Powerful Security Move: How This Could Change Everything

By **Kate O'Flaherty**

Screen sharing by the host only turned on by default

One of the major problems caused by Zoom bombers is the sharing of offensive images, sometimes containing pornography. To try and prevent this from happening, Zoom will make screen sharing privileges host only by default from May 9.

How to secure Zoom

Whether you love it, hate it, use it or don't, everyone has an opinion about Zoom. These new security features are great, but really, they should have been turned on by default from the start.

However, I don't see Zoom's issues as a reason to not use the service at all. In addition to these new security features, there are other things you can do to keep yourself as safe as possible while using the app. Firstly, don't use Zoom for any sensitive chats and [seek out an alternative](#) instead.

MORE FROM FORBES

Use Zoom? Here Are 7 Essential Steps You Can Take To Secure It

By Kate O'Flaherty

At the same time, be aware that when you are using Zoom, you need to [control your privacy](#)—services are free for a reason and there might be some data to have to give up.

When you do use Zoom, [you can ensure you are safer by not downloading the app where possible](#). In addition, [Zoom's surge in users means it's a target for phishing attacks](#). Be careful of any emails that claim they come from Zoom, they are often designed to steal your credentials.

The Evolving Role of Finance Chiefs

Sign up for The Balance Sheet, Forbes' biweekly newsletter from CFO Network Editor Ezequiel Minaya.

Follow me on [Twitter](#).



Kate O'Flaherty

Follow

I'm a freelance cybersecurity journalist with over a decade's experience writing news, reviews and features. I report and analyze breaking cybersecurity and privacy... **Read More**

[Site Feedback](#)

[Tips](#)

[Corrections](#)

[Reprints & Permissions](#)

[Terms](#)

[Privacy](#)

© 2020 Forbes Media LLC. All Rights Reserved.

[AdChoices](#)

ADVERTISEMENT
